**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

| | | |
|---|---|---|
| **IN RE: BPS DIRECT, LLC, AND CABELA'S, LLC, WIRETAPPING** | : | **MDL 3074** |
| | : | |
| | : | |
| | : | **E.D.Pa. ACTION NOS.:** |
| | : | **23-md-3074** |
| | : | **22-cv-4709** |
| | : | **23-cv-2282** |
| | : | **23-cv-2287** |
| | : | **23-cv-2293** |
| | : | **23-cv-2294** |
| | : | **23-cv-2295** |
| | : | **23-cv-2306** |
| | : | **23-cv-2338** |
| | : | **23-cv-4008** |

# MEMORANDUM

**KEARNEY, J.** **December 5, 2023**

We today address website users' challenges to retailers secretly tracking consumers' keystrokes and chosen webpages while browsing the retailers' websites. We put aside the rhetoric surrounding retailer marketing efforts versus surveillance. We must focus on the legal questions of whether website users suffer concrete injury from hidden tracking depending on what the retailer learns and, if so, whether the retailers' conduct in tracking their website users' conduct violates federal and state law.

The website users' first filed challenge through a Multi-District Litigation is to the use of session replay software embedded into two retailers' websites by third party vendors who then track the website user's conduct on the retailers' webpages as violating federal and several differing state wiretapping acts and a variety of common law torts grounded in privacy concepts. The second challenge arises closer to home with a Pennsylvania Facebook website user purchasing a gun from the same retailer who automatically discloses his purchase to Facebook which he claims

violates Pennsylvania's wiretapping act and the nondisclosure mandates in the Pennsylvania Uniform Firearms Act. Neither the session replay website users nor the Facebook website user allege either retailer accessed or shared their credit card, financial, or bank account data. They do not allege the retailers accessed or shared their private medical information. No website user alleges concrete specific injury arising from the retailers' use of software to track their browsing on the retailers' websites. Two website users focusing on session replay software and the Pennsylvania Facebook user generally plead they purchased products from a retailer's website. But even these three website users do not plead the retailers shared highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards.

The website users do not plead facts allowing us to find Article III standing. We grant the retailers' motions to dismiss with prejudice as to website users who cannot plead after two attempts disclosing personal credit card, financial, bank account or medical information possibly arising from a purchase from their websites. We grant the retailers' motions to dismiss without prejudice as to the two website users challenging session replay software and the Pennsylvania Facebook website user who allege they purchased a product from the websites but do not plead concrete injury through third party access to their highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards. We also dismiss without prejudice the Facebook website user's alternative claim of improper disclosure under the Pennsylvania Uniform Firearms Act.

## II. Alleged facts

BPS Direct, LLC and Cabela's, LLC own, manage, and operate physical retail stores known as Bass Pro Shops and Cabela's along with online websites which sell outdoor products, such as hunting gear and apparel, firearms, and camping equipment.[1] Bass and Cabela's maintain

a "Privacy Policy" and "Terms of Use and Community Guidelines" across their websites.[2] They place the Privacy Policy and Terms of Use on the homepages of their websites in smaller low-contrasting font at the bottom of the webpages.[3] Bass and Cabela's do not prompt website visitors to agree to or view the Privacy Policy or Terms of Use during their website visit.[4]

***Session replay code's function and scope.***

Third-party vendors including Microsoft, Quantum Metric, and Mouseflow, created session replay code computer software allowing website operators to record and playback an individual website visitor's browsing session and to view a website visitor's interactions on their websites in real-time.[5] Session replay code provides online marketers, advertisers, and website designers with specific insights into website visitor behavior which they can use to target website visitors with marketing and advertising content.[6]

Bass and Cabela's hire third-party vendors, called session replay providers, to create and deploy session replay code on their websites to track and analyze website visitors' activities.[7] The third party session replay providers embed snippets of JavaScript computer code in www.basspro.com and www.cabelas.com.[8] The embedded JavaScript computer code, or session replay code, then deploys on each website user's internet browser.[9] When a website visitor interacts with one of these two websites, for example by clicking on a button or scrolling down a web page, their browsers transmit electronic messages in the form of instructions to Cabela's and Bass's computer servers operating the website.[10] These messages instruct Bass and Cabela's what content is being viewed, clicked on, requested, and imputed by the user.[11] The website user's browser will "follow the code's instructions" by contemporaneously sending duplicate messages of the user's communications to the third party session replay provider.[12] This session replay code operates continuously during a user's visit to the Bass or Cabela's websites.[13]

Bass and Cabela's use session replay code to capture users' mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entries, and other forms of a user's navigation and interaction through their websites.[14] Session replay code can capture these events at hyper-frequent intervals, often just milliseconds apart.[15] Session replay code accumulates and transmits these events in blocks periodically throughout the visitor's website session.[16] The third party session replay providers store and control the data and can then interpret and replay the data.[17] Session replay providers use large swaths of data to visually recreate a website user's visit to a particular website, often through a video replay showing the website user's computer screen and the actions they took on the website.[18] Bass and Cabela's then use the data for commercial gain.[19]

Session replay code is capable of capturing nearly every action taken by a website visitor while they are on the website, including a visitor's personal or private sensitive data depending on what the visitor does while on the site.[20] Visible contents of website communications are transmitted to the third party session replay provider as Bass and Cabela's do not use masking configuration settings and their websites transmit all captured data to their session replay providers.[21]

Session replay code may capture information the visitor does not intend to submit to the website (for example, a user enters information in a text field and chooses not to click "submit") or information they intend to keep private using a private browser such as "Incognito Mode."[22] Session replay code may also permit Bass and Cabela's to view the interactions of visitors on their websites in real-time.[23] The data captured by session replay code will become known and visible to both the session replay provider and Bass and Cabela's.[24] But session replay code is not visible to a user who is navigating a webpage.[25]

Session replay providers aggregate and store website users' data under unique identifiers

called "fingerprints."[26] "Fingerprints" are unique to a particular user's combination of computer and browser settings, screen configuration, and other detectable information.[27] Session replay providers collect fingerprints across all of the sites they monitor.[28] If a user identifies themselves to one of these websites, the session replay provider can match the fingerprint with the user identity.[29] Session replay providers can then back-reference all of the user's web browsing activity across other websites previously visited, including websites where the user intended to remain anonymous.[30]

***The session replay Website Users' allegations.***

Eight persons bringing a consolidated class action complaint through the multi-district litigation accessed either the Bass or Cabela's website. These session replay Website Users Brian Calvert, Heather Cornell, Timothy Durham, Marilyn Hernandez, Peter Montecalvo, Greg Moore, Arlie Tucker, and Brittany Vonbergen did not know Bass and Cabela's embed session replay code on their websites.[31] Session replay Website Users transmitted communications to Bass and Cabela's website servers, including mouse clicks and movements, keystrokes, search terms, substantive information they inputted, pages they viewed, scroll movements, and copy and paste actions.[32] Session replay code automatically and instantaneously captured their acts and sent them to session replay providers.[33] Session replay providers created a unique ID and profile for each of the eight website users.[34] Bass and Cabela's did not include a pop-up disclosure, consent form, or privacy policy alerting them of Bass and Cabela's recording their visits through a third party.[35]

The eight session replay Website Users from five different states plead different browsing and purchasing experiences. Two session replay Website Users accessed the websites from California. Session replay Website User Durham accessed Cabela's website while in California.[36] Session replay Website User Moore also visited Bass's website on his computers and/or mobile

devices while in California.[37] Session replay Website User Hernandez visited Bass's website on her computer while in Maryland.[38] She browsed for jackets but did not purchase anything.[39] Session replay Website User Montecalvo consistently visited Cabela's website on his computer, smartphone, and iPad between 2010 through 2021 while in Massachusetts.[40] He made purchases during some of his visits.[41] He communicated with Cabela's by telling Cabela's what product he was interested in, what color light duty belt he wanted, and where he wanted the belt shipped.[42] He provided Cabela's with his name, address, and unpleaded payment and billing information during the checkout process.[43] Session replay Website User Tucker visited Bass's website on his mobile phone and computer while in Missouri.[44]

Three session replay Website Users accessed the websites in Pennsylvania. Website User Calvert visited Cabela's website to browse but did not purchase anything.[45] Session replay Website User Cornell visited Bass's website to browse and purchased a chair.[46] She informed Bass of the product she was interested in, what color chair she wanted, and where she wanted the chair shipped.[47] Session replay Website User Cornell provided her name, address, and unpleaded payment and billing information.[48] Session replay Website User Vonbergen visited Cabela's website on her computer and/or smartphone approximately four times while in Pennsylvania but did not plead purchasing products during the website use.[49]

***The Facebook Website User's allegations.***

Pennsylvanian David Irvin has a Facebook account and purchased a firearm from cabelas.com.[50] Bass and Cabela's disclosed to Facebook information he provided to them in connection with his purchase of the firearm, including his name, address, Facebook ID, and the type of gun he purchased.[51] Facebook Website User Irvin does not allege he entered payment or billing information on the Cabela's website.

Facebook Website User Irvin alleges Bass and Cabela's assisted Facebook with intercepting communications containing personally identifiable information and protected information about website visitors' firearms purchases using Facebook Tracking Pixel code.[52] Facebook Website User Irvin alleges Facebook Tracking Pixel code captures and transmits largely the same types of information as session replay code. Facebook Tracking Pixel is a piece of code advertisers like Bass and Cabela's can integrate into their website to track visitors' identities and interactions with their websites.[53] Facebook Tracking Pixel captures an action and sends a record to Facebook.[54] Facebook processes it, analyzes it, and assimilates it into datasets which it uses to target website visitors.[55] Bass and Cabela's websites host Facebook Tracking Pixel code configured to capture and transmit: (1) "PageView," which transmits the Uniform Resource Locators (URLs) accessed by visitors on Bass and Cabela's websites; (2) "ViewContent" which shows similar information but tracks users' access to pages for particular products; and (3) "Button Click Automatically Deleted," which tracks when users add a product, such as a firearm, to their cart and/or checkout.[56]

Facebook Tracking Pixel uses first- and third-party cookies.[57] Cookies are small blocks of data websites store on your computer. A first-party cookie is created by the website the user is visiting.[58] A third-party cookie is created by a different website than the one the user is visiting.[59] Facebook Tracking Pixel compels a user's browser to send cookies to Facebook when the user is visiting the Websites.[60] These cookies contain, among other things, the visitor's unencrypted Facebook ID and browser identifier.[61] These cookies combine the identifiers with the event data gathered by Facebook Tracking Pixel to determine the webpages visitors are visiting and the products they are purchasing.[62] Bass and Cabela's also use the "Advanced Matching" tool to find information on their websites containing users' first names, last names, and emails.[63] Bass and

Cabela's disclose this information to Facebook so it can match visitors to their Facebook profiles.[64] A Facebook user agrees to abide by Facebook's Terms of Service, Cookies Policy, and Data Policy.[65] Facebook represents through its policies and public statements it does not use sensitive personal data for ad targeting.[66]

## II. Analysis

The eight session replay Website Users bring this action individually and on behalf of a nationwide class and various state subclasses of all website users whose communications were intercepted through the use of session replay code embedded on Cabela's and Bass's websites.[67] Session replay Website Users allege Cabela's and Bass's conduct violates the Federal Wiretap Act, Computer Fraud and Abuse Act, California Invasion of Privacy Act, California Statutory Larceny, California Unfair Competition Law, Maryland Wiretapping and Electronic Surveillance Act, Massachusetts Wiretapping Statute, Missouri Wiretap Act, Missouri Merchandising Practices Act, and, Pennsylvania Wiretapping and Electronic Surveillance Control Act. They also claim the same conduct constitutes an invasion of privacy rights, trespass to chattels, and conversion to chattels under each relevant state's law.[68] Session replay Website Users seek compensatory, statutory, nominal, and/or punitive damages, restitution, declaratory and injunctive relief, pre-judgment and post-judgment interest, and attorneys' fees, costs, and expenses.[69]

Facebook Website User Irvin focuses on Facebook's role and seeks to represent a class of "all persons in Pennsylvania who have a Facebook account and who visited either cabelas.com, basspro.com or both."[70] Facebook Website User Irvin also seeks to represent a subclass defined as "all persons in Pennsylvania who have a Facebook account and who purchased a firearm from either cabelas.com, basspro.com or both."[71]

Cabela's and Bass move to dismiss the session replay Website Users' consolidated

complaint arguing: (1) session replay Website Users lack Article III standing because they do not adequately allege they suffered concrete injury or are likely to suffer the future harm of visiting Bass and Cabela's websites without their knowledge of session replay code, (2) session replay Website Users' various wiretap claims under state and federal law fail because both parties consented to the alleged interceptions and their allegations fail to meet several of the necessary elements to state a claim under the respective statutes; (3) session replay Website Users' invasion of privacy claims fail because they do not adequately allege (a) an intentional intrusion by Cabela's and Bass, (b) a reasonable expectation of privacy in the data collected, or (c) a "highly offensive" intrusion; (4) session replay Website Users fail to state a claim under the Computer Fraud and Abuse Act because they do not adequately allege Bass and Cabela's "accessed" their computers and mobile devices or caused any damage; (5) session replay Website Users lack statutory standing to bring a claim under the California Unfair Competition Law and fail to adequately allege an "unlawful" or "unfair" act by Bass and Cabela's; (6) session replay Website User Tucker's claim under the Missouri Merchandising Practices Act fails because session replay Website User Tucker does not allege (a) a "purchase;" (b) any alleged fraud was made "in connection with" any "merchandise;" or (c) he suffered an "ascertainable loss; (7) state law claims for conversion and trespass to chattels fail because session replay Website Users fail to allege a physical interference or the requisite intent; and (8) the statutory larceny claim fails because session replay Website Users do not allege the type of loss or the requisite intent.[72]

Bass and Cabela's separately moved to dismiss Facebook Website User Irvin's amended Complaint arguing: (1) Facebook Website User Irvin lacks Article III standing because he does not adequately allege he suffered concrete injury; (2) Facebook Website User Irvin does not state a claim under the Pennsylvania Wiretapping and Electronic Surveillance Control Act because he

(a) does not allege the interceptions took place in Pennsylvania, (b) does not allege several key elements under the statute, including an interception of "contents", and (c) consented to any supposed "interception" when he agreed to Facebook and Bass's policies.[73]

We dismiss all claims of session replay Website Users Durham, Calvert, Hernandez, Moore, Tucker, and Vonbergen with prejudice as they do not have standing and amendment would be futile given they have not plead a purchase or disclosure of financial information after two attempts. We dismiss the claims of session replay Website Users Cornell and Montecalvo and Facebook Website User Irvin without prejudice to timely filing amended Complaints if they can allege Bass and Cabela's intercepted their highly sensitive personal information such as financial data from banks or credit cards consistent with their obligations under Rule 11. We also dismiss Facebook Website User Irvin's claims under the non-disclosures mandates in the Pennsylvania Uniform Firearms Act without prejudice.

### A. Website Users do not plead Article III standing for the statutory and common law privacy and wiretapping claims.

Bass and Cabela's argue the session replay Website Users and Facebook Website User Irvin do not meet their burden to establish Article III standing because they do not adequately plead they suffered a concrete harm arising from their website visits.[74] Website Users counter they suffered harm bearing a close relationship to privacy torts which have been historically recognized as a basis for suit.[75]

We find session replay Website Users Durham, Calvert, Hernandez, Moore, Tucker, and Vonbergen lack standing because they do not allege they made purchases on the Websites or engaged in activity which would cause their browsers to send highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards to Bass or Cabela's. Session replay Website Users Cornell and Montecalvo and Facebook Website User

Irvin's allegations do not establish standing because they do not identify the personal information they inputted in the process of making purchases on the Websites. Session replay Website Users' fingerprinting allegations do not allow us to plausibly infer they suffered concrete harm. Session replay Website Users' remaining allegations of mental anguish and diminution of value are insufficient to confer standing.

We must first clarify the law to be applied to our standing analysis. The parties dispute what the Website Users are required to plead to establish standing to sue under a statute protecting against intangible harms. Website Users contend they have standing as long as they allege violations of statutes protecting against the same general types of harms traditionally recognized as the basis for lawsuits at common law.[76] Bass and Cabela's counter we must determine whether Website Users allege facts showing a harm closely related to the harm traditionally forming the basis of lawsuits at common law.[77] We find we must compare the nature of the harm alleged to analogous harms which were protected against at common law and determine whether there is a close enough relationship between the two to find concrete harm.

The Supreme Court's 2016 guidance in *Spokeo, Inc. v. Robins* instructs Website Users must allege Article III standing by pleading (1) they suffered an injury in fact, (2) fairly traceable to Cabela's and Bass's challenged conduct, and (3) likely to be redressed by a favorable judicial decision.[78] To establish injury in fact, Website Users must show they suffered "an invasion of a legally protected interest" which is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[79] "Standing allegations need not be crafted with precise detail, nor must the plaintiff prove his allegations of injury."[80]

Concrete does not mean tangible.[81] While tangible injuries are often easier to recognize, "[v]arious intangible harms can also be concrete," including "reputational harms, disclosure of

private information, and intrusion upon seclusion."[82] Intangible harms are concrete if they have "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts."[83]

An alleged violation of a statute is not enough to confer standing.[84] In *TransUnion v. Ramirez*, the Supreme Court emphasized the "important difference" between "(i) a plaintiff's statutory cause of action to sue a defendant over the defendant's violation of federal law, and (ii) a plaintiff's suffering concrete harm because of the defendant's violation of federal law."[85] An injury in law is different than an injury in fact. Congress may "create causes of action for plaintiffs to sue those who violate them," but "only plaintiffs who have shown that they suffered concrete harm by a defendant's statutory violation have standing to sue."[86] A risk of future harm, without more, does not establish standing in a suit for damages.[87]

"In the class action context, our standing inquiry focuses solely on the class representative(s)."[88] "That a suit may be a class action ... adds nothing to the question of standing, for even named plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong.'"[89]

The parties interpret the Supreme Court's 2021 teaching in *TransUnion* differently. Website Users focus on the section of the *TransUnion* opinion in which the Court explains Congress may "elevate to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law."[90] Website Users read the Court as saying all we must do to find concrete harm is determine whether the harm the statute protects against is *of the same general type* traditionally recognized as a basis for a lawsuit; if it is, then Congress may elevate the harm to a legally cognizable injury under the statute and we may find standing even if the *quantity or*

*extent* of the harm differs.[91] Website Users analogize their harms to the common law privacy-related torts of intrusion upon seclusion and public disclosure of private information.[92] Website Users argue because the wiretapping statutes protect against the same general type of harm as an invasion of privacy claim, all claims arising under the wiretapping statutes are based on concrete harm. Under Website Users' theory, the mere fact Cabela's and Bass recorded *any* information during their visits to the websites is enough to confer standing to sue.[93] Bass and Cabela's counter Website Users' allegations are not enough to establish injury post-*TransUnion* because allowing the standing inquiry to begin and end with the statutory violation "runs directly counter to the Supreme Court's clarification that a legislature's creation of a statutory prohibition or obligation and a cause of action does not relieve courts of their responsibility to independently decide whether a plaintiff has suffered a concrete harm under Article III."[94]

Website Users' interpretation runs counter to our Supreme Court's explicit guidance in *TransUnion*. In *TransUnion*, consumers alleged TransUnion put alerts on credit reports identifying individuals as potential terrorists based on a comparison of their first and last names to names on a list maintained by the United States Treasury.[95] Consumers alleged TransUnion violated the Fair Credit Reporting Act by failing to use reasonable procedures to ensure the accuracy of their credit files.[96] The Court assumed TransUnion violated its obligations under the Fair Credit Reporting Act to use reasonable procedures.[97] The Court nonetheless analyzed whether, based on the facts alleged, all class members suffered harm. The Court found only the 1,853 consumers whose reports containing misleading alerts were disseminated to third parties suffered concrete harm.[98] The Court reasoned, "[t]he mere existence of inaccurate information, absent dissemination, traditionally has not provided the basis for a lawsuit in American courts."[99] The Court found consumers who did not have their reports disseminated did not suffer concrete

harm.

The Court in *TransUnion* did not first look to see whether the harm the Act protects against is of the same *general type* as the harm protected at common law and then find all consumers had standing because they all alleged claims under the Act. The Court instead divided consumers into two groups for analytical purposes: (1) consumers whose information was disseminated to third parties, and (2) consumers whose information was not disseminated to third parties. The Court then independently analyzed the details of each group's factual allegations to assess whether the group's alleged harm had a "close relationship" to the harm traditionally recognized as providing a basis for a lawsuit. The mere fact TransUnion did not comply with reasonable procedures under the Act did not confer standing.

We face a similar analysis because the mere fact Website Users allege Cabela's and Bass intercepted electronic communications does not confer standing. We proceed as the Supreme Court instructs in *TransUnion* - first by grouping the Website Users based on the details of their alleged harms, and then by independently analyzing the details of their allegations to see whether they have a "close relationship" to a traditional harm.

We are guided by several thoughtful evaluations of similar claims over the past several months including from our colleague Judge Ranjan a little over three months ago in *Cook v. GameStop*.[100] Ms. Cook sued GameStop alleging GameStop's use of session replay on its website violated the same Pennsylvania wiretapping statute we are reviewing in part and the common law tort of intrusion upon seclusion.[101] Ms. Cook argued she had standing and Judge Ranjan need not analyze the sensitivity of the disclosed information because "there has been historical protection against 'the idea of somebody eavesdropping on you, somebody intruding on your privacy, regardless of what the intrusion yields them.'"[102] Ms. Cook contended the mere fact GameStop

recorded *any* information during her visit to its website is enough to give her standing to sue.[103] Judge Ranjan rejected this argument as "circular" because it "folds back onto a bare statutory violation."[104] Judge Ranjan, like we do, concluded under *TransUnion* he must examine the nature of the information intercepted to determine if it amounts to an invasion of historically protected privacy interests.[105]

Judge Andrews engaged in a similar analysis over eighteen months ago in *Massie v. General Motors LLC*, where Ms. Massie and Mr. Manglani challenged General Motors' use of session replay code on its website.[106] Like Ms. Cook, Ms. Massie and Mr. Manglani analogized their injuries to an invasion of privacy.[107] Judge Andrews granted General Motors' motion to dismiss finding Ms. Massie and Mr. Manglani lacked standing because they could not plead a "close relationship" between an invasion of privacy claim and "eavesdropping" on communications which do not involve personal information.[108]

Like Ms. Cook and Ms. Massie, Website Users look past our Supreme Court's critical directive a plead statutory violation does not relieve us of our duty to decide whether a Website User is harmed under Article III.[109] Even if the *type* of harm a statute is designed to protect resembles a *type* of harm traditionally protected, we cannot find harm where there is none. Website Users analogize their harms to intrusion upon seclusion and public disclosure of private facts – torts which require the interception or disclosure of private and personal information.[110] The protections which existed traditionally at common law existed only as to *private* information.[111]

Website Users' argument we must ignore the sensitivity of the intercepted content when considering standing does not withstand scrutiny. When asked during oral argument whether someone who has cabelas.com as their homepage suffers harm by merely loading their web browser and leaving it open, session replay Website Users' counsel responded, "I would say yes,

depending—because of the definition of electronic communication…it includes any nature of communication electronically."[112] Session replay Website Users' counsel continued, "[I]t depends on what the software would capture."[113] Session replay Website Users' counsel openly admitted the answer to the standing question "goes to content."[114] Website Users argue we must not consider the contents of the intercepted information but we also must consider the contents of the intercepted information. Website Users only want us to interpret harm *as Congress defines it under the statute*. But doing so leaves us with nothing but a bare statutory violation – which is not enough to confer standing under *TransUnion*.

Session replay Website Users contend Judge Ranjan in *Cook* and Judge Andrews in *Massie* erred in their standing analyses by requiring website visitors allege a privacy interest *identical* to the privacy right recognized at common law.[115] Session replay Website Users argue this interpretation is not in line with the Supreme Court's teachings since 2016 in *Spokeo* and its progeny, which only requires the interest protected by a statute bear a *close* relationship to a right traditionally recognized at common law.[116]

We disagree with the session replay Website Users' suggestion *Massie* and *Cook* are wrongly decided. Neither Judge Andrews nor Judge Ranjan required website visitors' privacy interests be identical to the right of privacy recognized at common law to establish standing. Both judges compared the harm alleged to analogous harms at common law and found there was not a close enough relationship between the two to find concrete harm.[117] This thoughtful parsing is precisely what the Supreme Court in *TransUnion* asks us to do.

We recognize many website visitors across the country are challenging the use of session replay code.[118] Most judges to consider the standing issue required website visitors "plead that the defendants' interception of their information amounts to 'an invasion of privacy interests that have

been historically protected' to satisfy the injury-in-fact element of Article III standing."[119] "These courts held where there are no allegations that the plaintiff shared personal or sensitive information on the website in question, the plaintiff has not adequately alleged a concrete harm to support Article III standing."[120]

Guided by our Supreme Court in *TransUnion* and our colleagues' reasoning in session replay decisions across the country, we now consider the sensitivity of the information Bass and Cabela's allegedly intercepted to determine "whether the interception of that kind of information amounts to an invasion of privacy interests that have been historically protected."[121]

While we recognize "standing is not dispensed in gross," we find Facebook Website User Irvin and session replay Website Users' alleged harm under the wiretapping statutes is the same as their alleged harm underlying their common law invasion of privacy claims.[122] We need not assess standing separately with respect to these claims. We assess Facebook Website User Irvin's standing under the Pennsylvania Uniform Firearms Act separately because this claim is based on slightly different disclosure conduct by Bass and Cabela's. We analyze standing on a website user-by-website user basis.

**1. Session replay Website User Durham lacks standing.**

Session replay Website User Durham alleges he accessed www.cabelas.com while in California.[123] He does not allege the types of interactions he had with Cabela's website or the specific information he disclosed on Cabela's website. He does not allege he browsed the website or even shared *any* information about himself. Mr. Durham does not even attempt to allege harm, much less harm which closely relates to the harm upon which intrusion upon seclusion or other privacy torts are based. We dismiss session replay Website User Durham's claims for lack of standing.

**2. Session replay Website Users Calvert, Hernandez, Moore, Tucker, and Vonbergen lack standing.**

Bass and Cabela's argue session replay Website Users who allege they did not purchase items on their websites lack Article III standing because they do not—and cannot—allege Bass and Cabela's captured anything other than their browsing activity and browsing activity is not sufficiently private to establish concrete harm.[124] Session replay Website Users counter their harm stems from the conduct of the wiretapping itself, regardless of the sensitivity of the content captured. We find session replay Website Users Durham, Calvert, Hernandez, Moore, Tucker, and Vonbergen cannot establish standing because they did not purchase items on the websites or engage in activity prompting their browsers to send sensitive personal information such as banking or credit card information to Bass or Cabela's.

Session replay Website Users allege Mr. Calvert, Ms. Hernandez, Mr. Moore, Mr. Tucker, and Ms. Vonbergen communicated with Cabela's and Bass's servers, which captured "mouse clicks and movements, keystrokes, search terms, substantive information inputted by [Website Users], pages and content viewed by [Website Users], scroll movement, and copy and paste actions."[125]

Session replay Website Users argue these allegations are sufficient to establish concrete harm because our Court of Appeals found unlawful tracking of internet activity satisfies Article III's "concrete harm" requirement in two decisions *In re Google* and *In re Nickelodeon*.[126] Both of these decisions predated the Supreme Court's 2021 teachings in *TransUnion.* Internet users sued internet advertising companies in *In re Google* under federal and state wiretapping and privacy laws alleging the advertising companies bypassed users' cookie blockers and placed tracking cookies on their personal computers.[127] The advertising companies used the tracking cookies to compile internet histories and create detailed profiles for each internet user.[128] The internet users

alleged Google bypassed the cookie blockers through deception and in contravention of its privacy policy which assured users its cookie blocker prevented the installation of tracking cookies.[129] Our Court of Appeals recognized internet users' standing, reasoning they "base their claims on highly specific allegations that the defendants, in the course of serving advertisements to their *personal* web browsers, implanted tracking cookies on their *personal* computers."[130]

In *In re Nickelodeon*, children sued Viacom and Google alleging they used cookies to unlawfully collect their personal information including their gender, birthdate, IP address, operating system, and browser version.[131] The children alleged Viacom and Google did this despite explicitly promising not to collect any personal information about children who browsed its websites.[132] The children also alleged the companies used "browser fingerprinting" to identify website visitors and link online and offline activity to identify specific users.[133] Our Court of Appeals five years before *TransUnion* reasoned the children's harm is concrete because it involves "a clear *de facto* injury, *i.e.*, the unlawful disclosure of legally protected information."

Cabela's and Bass counter the allegations in *Google* and *Nickelodeon* are distinguishable based on the type of information at issue in those cases.[134] Cabela's and Bass rely primarily on two session replay decisions in which our colleagues distinguished the allegations in *Google* and *Nickelodeon*.[135] In *Cook v. GameStop*, Judge Ranjan rejected Ms. Cook's argument she has standing under *Google* and *Nickelodeon*.[136] Judge Ranjan reasoned these decisions "might be abrogated by *TransUnion*" but are also distinguishable because they involved the capture of personal information – "registered account information in *Nickelodeon*, and tracking cookies embedded within the plaintiffs' personal computers and browsers in *Google*."[137] Judge Ranjan found Ms. Cook did not have standing to sue under the wiretapping statute because Ms. Cook did not enter any personally identifying information (e.g., name, address, credit card information)

which could connect her browsing activity to her.[138] Judge Ranjan found Ms. Cook still could not establish harm even if GameStop could tie her browsing activity to her because observing her product preferences "is no different from what GameStop employees would have been able to observe if Ms. Cook had gone into a brick-and-mortar store and began browsing the inventory."[139]

Cabela's and Bass also rely on Judge Andrews's analysis in *Massie* where Ms. Massie and Mr. Manglani browsed the vehicle sections of the website but did not purchase anything and did not input any of their personal information such as their zip codes, phone numbers, or email addresses.[140] Ms. Massie and Mr. Manglani relied on several cases, including *Google* and *Nickelodeon*, where judges identified invasion of privacy as an injury sufficient to confer standing.[141] Judge Andrews distinguished these authorities as they involved "the collection and disclosure of personal information," whereas Ms. Massie and Mr. Manglani did not allege the information collected was "personal or private within the common law understanding of a privacy right."[142] Judge Andrews granted the motion to dismiss for lack of standing.[143]

We find Website Users who did not disclose highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards cannot establish concrete harm. Both intrusion upon seclusion and public disclosure of private facts involve the interception or disclosure of private personal information in a highly offensive manner.[144] Although Website Users provide slightly more detail as to the actions taken by Mr. Calvert, Ms. Hernandez, Mr. Moore, Mr. Tucker, and Ms. Vonbergen, they do not allege these individuals disclosed highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards. Website Users merely allege session replay code captured "mouse clicks, keystrokes, pages and content viewed." This is no different than what Bass and Cabela's employees would have been able to observe if Website Users had gone into a brick-and-mortar

store and began browsing the inventory. Website Users do not have a personal privacy interest in their shopping activity.

We agree our Court of Appeals' pre-*TransUnion* analyses in *Nickelodeon* and *Google* are distinguishable.[145] Unlike the website visitors in those cases, Website Users Calvert, Hernandez, Moore, Tucker, and Vonbergen do not allege Bass or Cabela's intercepted private communications or personal information. Although Website Users allege session replay code captured "substantive information inputted," they do not plead the substantive information after two attempts. Website Users' vague allegations session replay providers collect their "highly personal information and substantive communications" do nothing to clarify the concreteness of harm.[146]

Website Users' allegations regarding the types of information session replay *can* capture are likewise insufficient. For example, session replay Website Users allege "if a website displays user account information to a logged-in user, that content *may be* captured by Session Replay Code" and "researchers have found that a variety of highly sensitive information *can be* captured in event responses from website visitors."[147] We need to know what session replay code actually captured, not what session replay code is capable of capturing.[148]

We are also guided by Judge White's reasoning in *Adams v. PSP Group*.[149] Ms. Adams sued Pet Supplies Plus alleging it used session replay code on its website to unlawfully intercept communications.[150] Ms. Adams did not make a purchase on the website.[151] She did not specify what information she shared on the website.[152] Pet Supplies moved to dismiss for lack of Article III standing.[153] Ms. Adams' analogized her harm to intrusion upon seclusion, which involves obtaining private, personal information about a person.[154] Judge White reasoned the question is "whether Plaintiff adequately alleges *facts* showing a harm that is closely related to the harm that forms the basis of the tort of intrusion upon seclusion."[155]

Judge White granted Pet Supplies' motion to dismiss for lack of standing because Ms. Adams did not allege she input sensitive, personal, or confidential information while on the website, she did not allege she made a purchase on the website, and she did not allege she shared any financial information such as credit card details.[156] Judge White reasoned, "A large portion of the Complaint is devoted to explaining Session Replay Code and its capabilities…But importantly, the Complaint does not allege or describe what information Plaintiff provided to Defendant while she was visiting its website."[157]

We join Judge White and our colleagues in finding website visitors do not have standing to sue under the wiretap statutes where they fail to identify the specific personal information captured by session replay code.[158] While we recognize "standing is not dispensed in gross," we find Facebook Website User Irvin and session replay Website Users' alleged harm under the wiretapping statutes is the same as their alleged harm underlying their common law invasion of privacy claims.[159] We need not assess standing separately with respect to these claims.

We are aware of Judge Chen's decision four weeks ago in *James v. Walt Disney* recognizing website visitors' standing based on browsing. Website users in *James* alleged the website's owner violated their privacy rights by embedding a third-party software on its website which captured and collected data as individuals browsed the website.[160] The website users alleged the intercepted information was not anonymized and included "specific web pages viewed, search terms entered, and purchase behavior."[161] Judge Chen found standing when they refer "to webpages viewed, searches conducted, purchase behavior, and so forth. That is enough to support standing."[162]

We disagree with Judge Chen's reasoning to the extent it suggests viewing activity, search activity, and purchase behavior is enough to establish concrete harm. Judge Chen relied on

precedent set by the Court of Appeals for the Ninth Circuit before it had the benefit of the Supreme Court's guidance in *TransUnion*.[163] We are guided instead by the law of standing following *TransUnion*.

Session replay Website Users Calvert, Hernandez, Moore, Tucker, and Vonbergen lack standing.

### 3. We grant session replay Website Users Cornell, Montecalvo, and Facebook Website User Irvin leave to amend to allege disclosure of credit card or financial information during their purchases.

Ms. Cornell, Mr. Montecalvo, and Mr. Irvin allege they purchased items on the Websites. But they do not plead what information they shared in the purchase.

Bass and Cabela's argue session replay Website Users Cornell and Mr. Montecalvo "fare no better" than the other session replay Website Users who did not make purchases because they only allege they entered basic personal information, which is not sufficiently private to confer standing.[164] Bass and Cabela's argue Facebook Website User Irvin cannot show he suffered concrete harm because he also did not disclose medical diagnosis information or financial data from banks or credit cards to Bass or Cabela's.[165] We find session replay Website Users Cornell and Montecalvo and Facebook Website User Irvin may be able to establish standing under the pleaded wiretap and privacy claims if they can truthfully allege Bass and Cabela's captured their highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards.

Session replay Website Users Cornell and Montecalvo allege they provided information to Bass and Cabela's by using their keyboards to enter their names, addresses, payment, and billing information when they made website purchases.[166] Ms. Cornell and Mr. Montecalvo also allege their website communications, which included "keystrokes (such as text being entered into an

information field or text box, both intentional and unintentional)", were "captured automatically and instantaneously by session replay code and sent to various Session Replay Providers."[167] Facebook Website User Irvin alleges Bass and Cabela's assisted Facebook in intercepting communications which contained "[his] name, address, Facebook ID, [and] gun he purchased, among other items."[168]

Unlike the other website users in the multi-district consolidated complaint, session replay Website Users Cornell and Montecalvo and Facebook Website User Irvin plausibly allege they entered personal information. Unlike website users in many of the other session replay cases around the country, session replay Website Users Cornell and Montecalvo and Facebook Website User Irvin allege session replay code captured more than simply their "shopping preferences," or information which could be revealed during a visit to Bass or Cabela's brick-and-mortar stores. Session replay Website Users Cornell and Montecalvo and Facebook Website User Irvin plead more than merely allege session replay *can* capture their personal information—they plausibly allege session replay code *did in fact* capture their personal information.

We find their allegations still fall short. We are not persuaded concrete injury exists merely because Bass and Cabela's disclosed Website Users' names and addresses. We are aware of two decisions in which judges held the disclosure of basic contact information such as names, addresses, and phone numbers inadequate to establish standing.[169] But we also note many of our colleagues deciding session replay standing issues have found significant the fact website visitors did not allege disclosure of information including names and addresses.[170] Case law is unclear on this point.

But Congress repeatedly advises us credit card data often warrants special protection under federal law.[171] Facebook Website User Irvin alleges he made a purchase, but he does not allege he

entered credit card details or other financial information. Although session replay Website Users Cornell and Montecalvo allege they disclosed "payment and billing information," they do not specifically allege Cabela's and Bass intercepted their credit card details.[172] Session replay Website Users Cornell and Montecalvo also do not allege whether the intercepted information is anonymized or encrypted. We are guided by our colleagues who found this allegation crucial to deciding whether a website visitor suffered concrete harm from session replay code.[173]

We grant session replay Website Users Cornell and Montecalvo and Facebook Website User Irvin leave to amend their statutory wiretap and common law privacy claims if they can truthfully allege Bass and Cabela's captured non-anonymized and unencrypted highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards.[174]

**4. Session replay Website Users' fingerprinting allegations do not allow us to plausibly infer they suffered concrete harm.**

Session replay Website Users allege session replay providers aggregated and stored their data under unique identifiers, or "fingerprints," which they can use to identify website users across other websites based on information entered on other websites.[175] Session replay Website Users contend these fingerprinting allegations are sufficient to confer standing under *In re Google*.[176] Bass and Cabela's argue browsing activity is not sufficiently personal or private to confer Article III standing.[177] We find session replay Website Users' fingerprinting allegations do not establish concrete harm.

We agree with session replay Website Users the fingerprinting allegations bear certain similarities to the allegations in *Google* and *Nickelodeon*, but we find those cases distinguishable. We are persuaded by Judge Conner's reasoning in *Farst v. Autozone*.[178] Matthew Farst sued AutoZone challenging its use of session replay code on its website under the Pennsylvania

wiretapping statute. Mr. Farst relied on *In re Nickelodeon* and *In re Google* in support of his standing argument.[179] Judge Conner reasoned Mr. Farst's reliance is "misplaced" because the manner of data collection and the type of data collected in those cases is different.[180] Judge Conner explained, "[t]hose cases involve defendants who deceived plaintiffs by secretly collecting their private data after promising they would not."[181] The type of data collected is different because unlike Mr. Farst, the website visitors in *Google* alleged Viacom and Google compiled internet-wide search histories and created detailed user profiles to serve targeted ads and the website visitors in *Nickelodeon* alleged internet advertising companies disclosed legally protected information.[182]

Unlike the website visitors in *Nickelodeon* and *Google*, session replay Website Users before us do not allege Bass or Cabela's deceived them or disclosed legally protected information. Session replay Website Users admit the Privacy Notices disclose they collect "browsing or search history, website interactions, and advertisement interactions" and then disclose the information "to service providers and others, such as advertising and analytics partners; affiliated companies; law enforcement."[183]

We find session replay Website Users' fingerprinting allegations do not establish concrete harm.

**5. Session replay Website Users' remaining allegations of mental anguish and diminution of value are insufficient to confer standing.**

Session replay Website Users claim Article III standing by alleging Bass and Cabela's caused them "mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications."[184] Bass and Cabela's argue we should dismiss these "threadbare assertions" as conclusory.[185] Session replay Website Users counter they need not prove mental anguish or suffering to establish standing.[186] Session replay Website Users also

argue "diminution of the value of private information is actionable."[187] We find session replay Website Users' vague allegations of mental anguish and diminution of value are not sufficient to establish concrete harm. Session replay Website Users cannot establish standing based on vague allegations of mental distress.[188] And "without particularized allegations the [plaintiffs'] Personal Information [was] actually accessed or misused, these plaintiffs cannot plausibly allege that their information suffered any decrease in value."[189]

We need not analyze session replay Website Users' harm separately under the wiretapping statutes and the privacy tort claims because the harm upon which all these claims are based is the same: Bass and Cabela's unlawful interception of their private information. We will analyze Facebook Website User Irvin's standing under the Uniform Firearms Act separately because his alleged harm is based on slightly different conduct – the disclosure of protected firearm purchase information.

### B. Facebook Website User Irvin lacks standing to sue under the nondisclosure mandates in the Pennsylvania Uniform Firearms Act.

Bass and Cabela's argue Facebook Website User Irvin cannot show he suffered concrete harm for his Pennsylvania Uniform Firearms Act claim because he does not allege he was affected by disclosure of his data to Facebook and he consented to Facebook's terms and Cabela's privacy policies.[190] Bass and Cabela's argue Facebook Website User Irvin lacks standing because he alleges Bass and Cabela's only disclosed his information to one entity—Facebook—and the tort of public disclosure of private facts requires publicity.[191] Facebook Website User Irvin counters he suffered concrete harm because Bass and Cabela's disclosed protected information about his firearms purchases.[192] We find Facebook Website User Irvin does not allege facts allowing us to plausibly infer he suffered concrete harm under Article III.

The Pennsylvania General Assembly, through the Pennsylvania Uniform Firearms Act,

provides in pertinent part:

> "All information provided by the potential purchaser, transferee or applicant, including, but not limited to, the potential purchaser, transferee or applicant's **name or identity, furnished by a potential purchaser** or transferee under this section or any applicant for a license to carry a firearm …**shall be confidential and not subject to public disclosure**."[193]

Facebook Website User Irvin alleges Bass and Cabela's violated the Uniform Firearms Act by disclosing his "[his] name, address, Facebook ID, [and] gun he purchased" to Facebook without his "knowledge, consent or express written authorization."[194] He analogizes his harm to the torts of public disclosure of private information and intrusion upon seclusion. We must determine whether his alleged harm has a "close relationship" to harms traditionally recognized as the basis for lawsuits at common law.

Bass and Cabela's rely primarily on *Barclift v. Keystone Credit Services* in support of their position Facebook Website User Irvin lacks standing.[195] Keystone hired a mailing vendor to print and send Ms. Barclift a letter notifying her Keystone intended to collect a debt.[196] Ms. Barclift sued Keystone under the Fair Debt Collections Practices Act for sharing her personal information with the mailing vendor.[197] Judge Leeson reasoned her alleged harm most closely resembles the common law claim of public disclosure of private facts.[198] One of the elements of the tort is publicity of private facts. Judge Leeson reasoned because Ms. Barclift did not allege Keystone shared her information with a larger group of people, her alleged injury does not bear a close relationship to the tort.[199]

Facebook Website User Irvin counters his claim is analogous to the tort of intrusion upon seclusion which does not require publicity.[200] Facebook Website User Irvin relies on case law arising under the federal Video Privacy Protection Act and Michigan's Preservation of Personal Privacy Act in support of his position.[201] Facebook Website User Irvin argues, "[a]s with the

[Video Privacy Protection Act] and the [Preservation of Personal Privacy Act], the [Uniform Firearms Act] deems a type of information 'confidential' and prohibits its 'disclosure.'"[202] Facebook Website User Irvin claims because Bass and Cabela's disclosed his information in violation of the Uniform Firearms Act, he suffered an intangible harm akin to intrusion upon seclusion.[203]

We recognize Facebook Website User Irvin's argument bears some resemblance to standing arguments arising under cases addressing the Video Privacy Protection Act and Michigan's Protection of Personal Privacy Act. But the Supreme Court in *TransUnion* teaches we must analyze the alleged harm—not the statute—to determine whether Facebook Website User Irvin has standing.[204] We proceed as the Court instructs us in *TransUnion*: first by analyzing the details of the alleged harm, and then by determining whether the allegations have a "close relationship" to a traditional harm.

We agree Facebook Website User Irvin cannot establish harm using the analog of public disclosure of private facts because this tort requires publicity. "To recover damages for disclosure of private information a plaintiff must allege the matter publicized is (1) publicity, given to (2) private facts, (3) which would be highly offensive to a reasonable person, and (4) is not of legitimate concern to the public."[205] Facebook Website User Irvin alleges only one party—Facebook—received his information. He does not allege widespread disclosure or disclosure "to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."[206] Public disclosure of private facts is not a proper analog.

Facebook Website User Irvin analogizes his harm to intrusion upon seclusion. We again note the disclosure of basic personal information does not necessarily confer standing. Facebook Website User Irvin also alleges Bass and Cabela's disclosed his Facebook ID and his gun purchase.

The retailers' disclosure of Facebook Website User Irvin's Facebook ID *to Facebook* is hardly intrusive. We find disclosing a gun purchase is not the type of highly offensive or objectionable conduct to which liability can attach. After Facebook Website User Irvin made his online gun purchase, he needed to pick up the firearm at a store.[207] Other shoppers and employees of Cabela's would identify Facebook Website User Irvin and observe his gun purchase. "The difference in fora between online and in-person shopping outlets does not transform the generally public nature of shopping into a 'private affair.'"[208] We find the information Bass and Cabela's allegedly disclosed to Facebook—name, address, Facebook ID, and gun purchase—is not sufficiently private to confer standing.[209]

We dismiss Facebook Website User Irvin's claim under the Pennsylvania Uniform Firearms Act with leave to amend if he can allege Facebook Tracking Pixel captured non-anonymized and unencrypted highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards.

**C. Website Users do not have standing to assert claims for injunctive relief.**

Website Users ask us to enjoin Cabela's and Bass from "continuing the unlawful practices described herein" and prevent the future interceptions of communications.[210] Cabela's and Bass contend Website Users lack standing to pursue a claim for injunctive relief because injunctions protect against future harm and Website Users cannot contend they will suffer the future harm of visiting the websites with session replay running without their knowledge.[211] Website Users counter they have standing because Bass and Cabela's continue to employ session replay code and they suffer continuing adverse effects.[212] We find Website Users do not have standing to seek injunctive relief because they do not plausibly allege they are likely to suffer future injury from Bass or Cabela's conduct.

Standing "is not dispensed in gross;" it must be shown "for each claim . . . and for each form of relief [sought] (for example, injunctive relief and damages)."[213] In order to have standing to seek injunctive relief, Website Users must establish they are "likely to suffer future injury" from Bass and Cabela's conduct.[214] "[A] plaintiff must demonstrate "continuing, present adverse effects" and may not rely solely on "[p]ast exposure to illegal conduct."[215] Instead, they must show a real and immediate threat of repeated future injury in order to satisfy the "injury in fact" requirement of Article III.[216]

Bass and Cabela's rely in part on a decision of our Court of Appeals in *McNair v. Synapse Group*.[217] Former customers of a magazine sued a magazine marketing company for consumer fraud alleging the marketing company sold subscriptions in an unlawfully deceptive way.[218] Our Court of Appeals held the magazine customers did not have standing to seek injunctive relief reasoning any future injury is "wholly conjectural" because the former customers were already aware of Synapse's advertising practices.[219] The Court of Appeals explained, "[T]he law accords people the dignity of assuming that they act rationally, in light of the information they possess."[220]

Bass and Cabela's also rely on our Court of Appeals' decision in *In re Johnson & Johnson Talcum Powder Litigation*.[221] In *In re Johnson & Johnson*, Ms. Estrada alleged a Johnson & Johnson product increased the risk of developing ovarian cancer. Ms. Estrada asserted she suffered an economic injury by purchasing improperly marketed Baby Powder.[222] She sought to enjoin the manufacturer of the baby powder product from continuing to sell baby powder without warning customers of the alleged health risks.[223] Our Court of Appeals held Ms. Estrada did not have standing to seek injunctive relief, reasoning, "Because Estrada makes clear in this very lawsuit that she is well aware of health risks associated with using Baby Powder, we readily conclude that she is not likely to suffer future economic injury."[224] The Court of Appeals explained the fact Ms.

Estrada is aware of the health risks is fatal to her suit for failure to warn of certain health risks because Ms. Estrada cannot "possibly be deceived again into buying Baby Powder without being aware of those same risks."[225]

Website Users counter the *interception*, rather than the lack of awareness Bass and Cabela's are tracking them, is the injury.[226] Website Users rely on *Brown v. Google* in support of their argument they have standing to seek injunctive relief.[227] Website visitors sued Google for its "surreptitious interception and collection of personal and sensitive user data while users are in 'private browsing mode.'"[228] Website visitors sought to enjoin Google from intercepting, tracking, or collecting class members' communications after class members used a browser while in "private browsing mode."[229] Google sought summary judgment on the basis the website visitors could not show the risk of harm is sufficiently imminent and substantial to confer standing. Judge Gonzalez Rogers disagreed and denied summary judgment, reasoning, "Google's conduct has not stopped. Plaintiffs have demonstrated that absent an injunction, Google will continue to collect users' private browsing data for its own use without users' express consent."[230]

We note Website Users' authority is from the Court of Appeals for the Ninth Circuit reviewing a summary judgment analysis of much different facts on a developed record in which website visitors demonstrated Google would continue to collect private browsing data without user consent absent an injunction.[231] As Judge Gonzalez Rogers notes in her opinion, "[T]he standing analysis is contextual."[232] This case arises in a different context. As a federal district court sitting in Pennsylvania reviewing a motion to dismiss, we are bound to follow the precedent set forth by the Third Circuit.

We find our Website Users are not likely to suffer future injury from Bass or Cabela's conduct. Website Users allege Bass and Cabela's used a third party to track their movements on

the websites without their knowledge. Website Users brought this lawsuit and are presumably now aware of the alleged risks associated with browsing Cabela's and Bass's websites.[233] Website Users' activity on Bass and Cabela's websites is entirely voluntary and we assume Website Users will act rationally in light of the information they possess.[234] They may visit Cabela's or Bass's website again, but they will do so with the knowledge session replay is capturing their movements. "Pleading a lack of self-restraint may elicit sympathy but it will not typically invoke the jurisdiction of a federal court."[235] Website Users will not be deceived again in the future.

We dismiss Website Users' claims for injunctive relief because Website Users do not allege they are "likely to suffer future injury" from Bass and Cabela's conduct.[236]

## III. Conclusion

Session replay Website Users Durham, Calvert, Hernandez, Moore, Tucker, and Vonbergen cannot establish concrete harm after two attempts because they did not make purchases on the Websites or engage in any activity prompting their browsers to send highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards to Bass or Cabela's. We dismiss their claims with prejudice because they lack standing. We afforded Ms. Vonbergen, Mr. Moore, Jr., Mr. Calvert, Mr. Tucker, Mr. Durham, and Ms. Hernandez two chances to state a claim. Case law in this area, while evolving, recognized the website users must be able to plead facts of sharing highly sensitive personal information such as a medical diagnosis or financial data from banks or credit cards to enjoy Article III standing. We dismiss their statutory and common law claims with prejudice because all named Website Users asserting claims under those laws lack standing.[237]

Session replay Website Users Cornell and Montecalvo and Facebook Website User Irvin do not establish concrete harm because they do not identify the information Bass and Cabela's

allegedly intercepted during their purchasing activity. We dismiss their claims without prejudice to their timely filing amended Complaints if they can truthfully allege Bass and Cabela's intercepted and shared highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards under Rule 11 during their interactions (including the alleged purchase) on the website. We dismiss the statutory and common law claims arising under federal law and the laws of Pennsylvania and Massachusetts without prejudice.[238]

---

[1] ECF No. 53 ¶¶ 26, 88.

[2] *Id.* ¶¶ 155, 157.

[3] *Id.* ¶¶ 155-157.

[4] *Id.* ¶¶ 156-157.

[5] *Id.* ¶¶ 5, 7.

[6] *Id.* ¶¶ 31, 64.

[7] *Id.* ¶¶ 1-2, 89.

[8] *Id.* ¶ 1.

[9] *Id.*

[10] *Id.* ¶ 66.

[11] *Id.*

[12] *Id.* ¶ 67.

[13] *Id.* ¶ 142.

[14] *Id.* ¶ 68.

[15] *Id.*

[16] *Id.*

[17] *Id.* ¶ 70.

[18] *Id.* ¶ 3.

[19] *Id.* ¶ 183.

[20] *Id.* ¶ 65.

[21] *Id.* ¶ 69.

[22] *Id.* ¶¶ 65, 74.

[23] *Id.* ¶ 7.

[24] *Id.* ¶ 76.

[25] *Id.* ¶ 92. Session replay code can only be identified by technical users who understand web technologies and can enable alternative display modes showing the underlying HTML containing the code. *Id.* ¶ 93.

[26] *Id.* ¶ 47.

[27] *Id.* ¶ 79.

[28] *Id.*

[29] *Id.* ¶ 80.

[30] *Id.*

[31] *Id.* ¶ 137.

[32] *Id.* ¶¶ 99, 105, 111, 118, 123, 128, 133.

[33] *Id.* ¶ 138.

[34] *Id.* ¶ 139.

[35] *Id.* ¶¶ 101, 107, 113, 120, 125, 130, 135.

[36] ECF No. 53 ¶ 12.

[37] *Id.* ¶ 122.

[38] *Id.* ¶ 109.

[39] *Id.* ¶¶ 109-110.

[40] *Id.* ¶¶ 115-116.

[41] *Id.* ¶ 117.

[42] *Id.*

[43] *Id.*

[44] *Id.* ¶ 127.

[45] *Id.* ¶¶ 97-98.

[46] *Id.* ¶¶ 103-104.

[47] *Id.* ¶ 104.

[48] *Id.*

[49] *Id.* ¶ 132.

[50] *Id.* ¶ 6.

[51] *Id.* ¶ 70.

[52] *Irvin* ECF No. 20 ¶¶ 2, 9.

[53] *Id.* ¶ 14.

[54] *Id.*

[55] *Id.* ¶¶ 12-14.

[56] *Id.* ¶¶ 17-25.

[57] *Id.* ¶ 27.

[58] *Id.*

[59] *Id.*

[60] *Id.* ¶ 28.

[61] *Id.* ¶¶ 29-30.

[62] *Id.* ¶ 31.

[63] *Id.* ¶ 32.

[64] *Id.* ¶ 33.

[65] *Id.* ¶ 40.

[66] *Id.* ¶¶ 42-46.

[67] ECF No. 53 ¶¶ 9, 158. Session replay Website Users bring state subclass actions on behalf of website users in California, Maryland, Massachusetts, Missouri, and Pennsylvania whose communications were intercepted using session replay code embedded on Bass and Cabela's websites.

[68] *Id.* ¶¶ 8, 167-476.

[69] *Id.* ¶ 9, Request for Relief ¶¶ C-H.

[70] *Irvin* ECF No. 20 ¶ 49.

[71] *Id.*

[72] ECF No. 54-1. Bass and Cabela's challenge the sufficiency of the fact allegations in Website Users' complaints. Website Users must state a claim upon which relief can be granted to proceed beyond a motion to dismiss. Fed. R. Civ. P. 12(b)(6). The purpose of Rule 12(b)(6) is to test the sufficiency of the factual allegations in a complaint. *Sanders v. United States*, 790 F. App'x 424, 426 (3d Cir. 2019). If a plaintiff is unable to plead "enough facts to state a claim to relief that is plausible on its face," the court should dismiss the complaint. *Id.* (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)); *see also Kajla v. U.S. Bank Nat'l Ass'n as Tr. for Credit Suisse First Boston MBS ARMT 2005-8*, 806 F. App'x 101, 104 n.5 (3d Cir. 2020) (quoting *Warren Gen. Hosp. v. Amgen Inc.*, 643 F.3d 77, 84 (3d Cir. 2011)). "A claim is facially plausible 'when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.'" *Klotz v. Celentano Stadtmauer and Walentowicz LLP*, 991 F.3d 458, 462 (3d Cir. 2021) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). While "[t]he plausibility standard is not akin to a 'probability requirement,'" it does require the pleading show "more than a sheer possibility … a defendant has acted unlawfully." *Riboldi v. Warren Cnty. Dep't of Human Servs. Div. of Temp. Assistance & Soc. Servs.*, 781 F. App'x 44, 46 (3d Cir. 2019) (quoting *Iqbal*, 556 U.S. at 678). "A pleading that merely 'tenders naked assertion[s] devoid of further factual enhancement' is insufficient." *Id.* (quoting *Iqbal*, 556 U.S. at 668).

In determining whether to grant a Rule 12(b)(6) motion, "we accept all well-pleaded allegations as true and draw all reasonable inferences in favor of the plaintiff" but "disregard threadbare recitals of the elements of a cause of action, legal conclusions, and conclusory statements." *Robert*

*W. Mauthe, M.D., P.C. v. Spreemo, Inc.*, 806 F. App'x 151, 152 (3d Cir. 2020) (quoting *City of Cambridge Ret. Sys. v. Altisource Asset Mgmt. Corp.*, 908 F.3d 872, 878–79 (3d Cir. 2018)). Our Court of Appeals requires us to apply a three-step analysis to a 12(b)(6) motion: (1) we "'tak[e] note of the elements a plaintiff must plead to state a claim'"; (2) we "identify allegations that … 'are not entitled to the assumption of truth' because those allegations 'are no more than conclusion[s]'"; and, (3) "'[w]hen there are well-pleaded factual allegations,' we 'assume their veracity' … in addition to assuming the veracity of 'all reasonable inferences that can be drawn from' those allegations … and, construing the allegations and reasonable inferences 'in the light most favorable to the [plaintiff]'…, we determine whether they 'plausibly give rise to an entitlement to relief.'" *Oakwood Lab'ys LLC v. Thanoo*, 999 F.3d 892, 904 (3d Cir. 2021) (internal citations omitted); *Connelly v. Lane Constr. Corp.*, 809 F.3d 780, 787 (3d Cir. 2016).

Bass and Cabela's also make a jurisdictional challenge under Federal Rule 12(b)(1). A Rule12(b)(1) challenge can be either a facial or factual attack. *Davis v. Wells Fargo*, 824 F.3d 333, 346 (3d Cir. 2016). A facial challenge is reviewed like a 12(b)(6) motion, requiring us to consider all allegations of the complaint to be true. *Hartig Drug Co., Inc. v. Senju Pharm. Co.*, 836 F.3d 261, 268 (3d Cir. 2016). A factual attack, on the other hand, does not give the plaintiff the presumption of truth and instead allows "a court [to] weigh and consider evidence outside the pleadings." *Id.* (citations and quotations omitted). Bass and Cabela's make a facial attack.

[73] *Irvin* ECF No. 39.

[74] ECF No. 54-1 at 14-16; *Irvin* ECF No. 39 at 12-15.

[75] ECF No. 56 at 16-19; *Irvin* ECF No. 47 at 7.

[76] ECF No. 56 at 18 ("Thus, so long as the underlying *type* of harm is similar, the *quantity or extent* of the harm need not be the same.") (emphasis in original).; ECF No. 73 at 20:20-22:8.

[77] ECF No. 57 at 12 ("Accordingly, to determine whether Plaintiffs have standing to bring their claims, the Court here must determine 'whether Plaintiff[s] adequately allege facts showing a harm that is closely related to the harm that forms the basis of the tort of intrusion upon seclusion.'") (quoting *Adams v. PSP Grp., LLC*, No. 22-1210, 2023 WL 5951784, *6 (E.D. Mo.)).

[78] *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992)); *Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000)).

[79] *Spokeo*, 578 U.S. at 339 (citing *Lujan*, 504 U.S. at 560).

[80] *Baur v. Veneman*, 352 F.3d 625, 631 (2d Cir. 2003).

[81] *Spokeo*, 578 U.S. at 340.

[82] *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021).

[83] *Id.* at 2204.

[84] *Spokeo*, 578 U.S. at 341 (2016) ("Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation.").

[85] *TransUnion*, 141 S. Ct. at 2205.

[86] *Davis v. Universal Prot. Servs., LLC*, 558 F. Supp. 3d 220, 224 (E.D. Pa. 2021) (citations omitted).

[87] *Id.*

[88] *Mielo v. Steak 'N Shake Operations, Inc.*, 897 F.3d 467, 478 (3d Cir. 2018).

[89] *Spokeo*, 578 U.S. at 338 (citations omitted).

[90] *TransUnion*, 141 S. Ct. at 2205. Website Users also rely on a pre-*TransUnion* United States Court of Appeals for the Seventh Circuit decision for this proposition. *See Gadelhak v. AT&T Services, Inc.*, 950 F.3d 458, 462 (7th Cir. 2020).

[91] ECF No. 56 at 18; ECF No. 73 at 20:20-21:6.

[92] ECF No. 56 at 17.

[93] ECF No. 73 at 23:8-24:6.

[94] ECF No. 57 at 9-10.

[95] *TransUnion*, 141 S. Ct. at 2197.

[96] *Id.*

[97] *Id.* at 2208 ("Assuming that the plaintiffs are correct that TransUnion violated its obligations under the Fair Credit Reporting Act to use reasonable procedures in internally maintaining the credit files, we must determine whether the 8,185 class members suffered concrete harm from TransUnion's failure to employ reasonable procedures.").

[98] *Id.*

[99] *Id.* at 2197.

[100] *Cook v. GameStop, Inc.*, No. 22-1292, 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023).

[101] *Id.* at *1.

[102] *Id.* at *3.

[103] *Id.*

[104] *Id.*

[105] *Id.* at *4.

[106] *Massie v. Gen. Motors LLC*, No. 21-0787, 2022 WL 534468 (D. Del. Feb. 17, 2022).

[107] *Id.* at *3.

[108] *Id.* at *5 ("'Eavesdropping' on communications that do not involve personal information, personally identifiable information, or information over which a party has a reasonable expectation of privacy does not amount to a concrete injury.").

[109] *TransUnion*, 141 S. Ct. at 2205.

[110] Website Users analogize their harms to the common law privacy-related torts of intrusion upon seclusion and public disclosure of private information. ECF No. 56 at 17. "Intrusion upon seclusion involves obtaining or intercepting private, personal communications or information about a person in a matter that is highly offensive or unreasonable." *Adams*, 2023 WL 5951784, at *7. Disclosure of private information involves "(1) publicity, given to (2) private facts, (3) which would be highly offensive to a reasonable person, and (4) is not of legitimate concern to the public." *Farst v. AutoZone, Inc.*, No. 22-1435, 2023 WL 7179807, at *4 (M.D. Pa. Nov. 1, 2023) (internal citations and quotations omitted).

[111] *U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").

[112] ECF No. 73 at 27:12-23.

[113] *Id.* at 28:6-14.

[114] *Id.* at 28:15-20.

[115] ECF No. 56 at 21.

[116] *Id.*

[117] *Cook*, 2023 WL 5529772, at *4 ("[T]he Court must examine the nature of the information that GameStop allegedly intercepted and determine whether the interception of that kind of information amounts to an invasion of privacy interests that have been historically protected."); *Massie*, 2022

WL 534468, at *3 ("Here, Plaintiffs do not allege that any of their information collected by the Session Replay software was personal or private within the common law understanding of a privacy right. Therefore, I find Plaintiffs have not suffered a concrete injury because they do not have a privacy interest at stake.").

[118] *See, e.g., Farst v. AutoZone, Inc.*, No. 22-1435 (M.D. Pa.); *In re Zillow Grp., Inc. Session Replay Software Litig.*, No. 22-1282 (W.D. Wash.); *Popa v. PSP Grp., LLC*, No. 23-294 (W.D. Wash.); *Adams v. PSP Grp., LLC*, No. 22-1210 (E.D. Mo.); *Jones v. Bloomingdales.com, LLC*, No. 22-1095, 2023 (E.D. Mo.); *Cook v. GameStop, Inc.*, No. 22-1292 (W.D. Pa.); *Massie v. Gen. Motors LLC*, No. 21-787 (D. Del.); *Lightoller v. Jetblue Airways Corp.*, No. 23-361 (S.D. Cal.); *Mikulsky v. Noom, Inc.*, No. 23-285 (S.D. Cal.); *Straubmuller v. Jetblue Airways Corp.*, No. 23-384 (D. Md.); *James v. Walt Disney Co.*, No. 23-2500 (N.D. Cal.); *Thomas v. Papa Johns Int'l, Inc.*, No. 22-2012 (S.D. Cal.); *Toston v. JetBlue Airways Corp.*, No. 23-1156 (C.D. Cal.).

[119] *In re Zillow Grp., Inc. Session Replay Software Litig.*, No. 22-1282, 2023 WL 5916559, at *1 (W.D. Wash. Sept. 11, 2023).

[120] *Adams*, 2023 WL 5951784, at *7 n. 4.

[121] *Cook*, 2023 WL 5529772, at *4.

[122] *Town of Chester, N.Y. v. Laroe Estates, Inc.*, 581 U.S. 433, 439 (2017).

[123] ECF No. 53 ¶ 12.

[124] ECF No. 54-1 at 15.

[125] ECF No. 53 ¶¶ 99, 111, 123, 128, 133.

[126] ECF No. 56 at 20. *See In re Google Inc. Cookie Placement Cons. Priv. Litig.*, 934 F.3d 316 (3d Cir. 2019); *In re Nickelodeon Cons. Priv. Litig.*, 827 F.3d 262 (3d Cir. 2016).

[127] 806 F.3d 125 (3d Cir. 2015).

[128] *Id.* at 131.

[129] *Id.* at 132.

[130] *Id.* at 134-35. After the decision in *Spokeo*, our Court of Appeals addressed the internet users' standing again in *In re Google Inc. Cookie Placement Cons. Priv. Litig.*, 934 F.3d 316 (3d Cir. 2019) and upheld standing. Our Court of Appeals recognized internet users still have standing post-*Spokeo*, finding, "History and tradition reinforce that a concrete injury for Article III standing purposes occurs when Google, or any other third party, tracks a person's internet browser activity without authorization." *Id.* at 325.

[131] 827 F.3d 262 (3d Cir. 2016).

[132] *Id.* at 267.

[133] *Id.* at 270.

[134] ECF No. 57 at 11-12.

[135] *Id.*

[136] *Cook*, 2023 WL 5529772, at *5.

[137] *Id.*

[138] *Id.*

[139] *Id.*

[140] *Massie*, 2022 WL 534468, at *2.

[141] *Id.* at *3-4.

[142] *Id.*

[143] *Id.* at *5 ("'Eavesdropping' on communications that do not involve personal information, personally identifiable information, or information over which a party has a reasonable expectation of privacy does not amount to a concrete injury.").

[144] "Intrusion upon seclusion involves obtaining or intercepting private, personal communications or information about a person in a matter that is highly offensive or unreasonable." *Adams*, 2023 WL 5951784, at *7. Disclosure of private information involves "(1) publicity, given to (2) private facts, (3) which would be highly offensive to a reasonable person, and (4) is not of legitimate concern to the public." *Farst v. AutoZone, Inc.*, No. 22-1435, 2023 WL 7179807, at *4 (M.D. Pa. Nov. 1, 2023) (internal citations and quotations omitted).

[145] Cabela's and Bass suggest these cases may be abrogated by *TransUnion*, which clarified lone statutory violations are not enough to establish standing. ECF No. 57 at 11-12. We need not decide this today because even if they are not abrogated by *TransUnion*, they are distinguishable.

[146] ECF No. 53 ¶ 91.

[147] *Id.* at ¶¶ 73, 77; *see also*, ¶ 65 ("Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data…").

[148] *See Straubmuller*, 2023 WL 5671615, at *4 ("Here, it is dispositive that Plaintiff only alleges that Session Replay Code could capture personal information, not that it actually captured Plaintiff's personal information.").

[149] *Adams*, 2023 WL 5951784.

[150] *Id.* at *2.

[151] *Id.*

[152] *Id.*

[153] *Id.* at *5.

[154] *Id.* at *6.

[155] *Id.* (emphasis added).

[156] *Id.* at *7.

[157] *Id.*

[158] *See Straubmuller*, 2023 WL 5671615, at *4 ("Because the Complaint says nothing about the kinds of interactions Plaintiff had with Defendant's website, much less the specific kinds of captured personal information implicating a substantive privacy interest, Plaintiff has not alleged that his personal information was intercepted and recorded by Defendant."); *Mikulsky*, 2023 WL 4567096, at *5 ("To survive a motion to dismiss, a plaintiff must identify the 'specific personal information she disclosed that implicates a protectable privacy interest.'") (citations omitted).

[159] *Town of Chester, N.Y. v. Laroe Estates, Inc.*, 581 U.S. 433, 439 (2017).

[160] No. 23-2500, 2023 WL 7392285 (N.D. Cal. Nov. 8, 2023). Although website visitors in *James v. Walt Disney* do not characterize the third-party software as "session replay," they allege the third party embeds code into websites without visitors' knowledge and then instructs the user's browser to send certain captured data points to the third party for analysis of consumer behavior. *Id.* at *1, 14-15.

[161] *Id.* at *5.

[162] *Id.* at *7. Judge Chen also recognized "simply referring to keystrokes, mouse clicks, and "other communications" – without additional allegations – would standing alone arguably be insufficient" to demonstrate Article III standing. *Id.*

[163] *Id.* at *5-6. Judge Chen relied on the decision of the Court of Appeals for the Ninth Circuit in *In re Facebook, Inc. Internet Tracking Litig.*, where the court of appeals held website visitors established standing because Facebook's tracking practices allowed it to gather an individual's

likes, dislikes, and habits over a significant amount of time "without affording users a meaningful opportunity to control or prevent the unauthorized exploration of their private lives." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598-99 (9th Cir. 2020). Judge Chen reasoned *Facebook* involved more personal information than the allegedly intercepted information in the case before him. *Id.* at *6.

[164] ECF No. 54-1 at 15-16.

[165] *Irvin* ECF No. 52 at 3.

[166] ECF No. 53 ¶¶ 104, 117.

[167] *Id.* at ¶¶ 1, 138.

[168] *Irvin* ECF No. 20 ¶ 70.

[169] *See I.C. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049-50 (N.D. Cal. 2022) (finding disclosure of "basic contact information, including one's email address, phone number, or . . . username" inadequate to establish standing); *Brignola v. Home Properties, L.P.*, No. 10-3884, 2013 WL 1795336, at *12 (E.D. Pa. Apr. 26, 2013) (finding a plaintiff's "name, address, phone number, etc. . . . are not private facts actionable for an [invasion of privacy] claim").

[170] *See Farst v*, 2023 WL 7179807, at *5 ("Farst does not aver AutoZone disclosed his home address, credit card, bank account, social security number, or any other information that could potentially be used to identify him or materially increases his risk of future harm."); *Cook*, 2023 WL 5529772, at *4 ("Ms. Cook did not enter any personally identifying information at any point during her interaction. Not her name. Not her address. Not her credit card information."); *Adams*, 2023 WL 5951784, at *7 (E.D. Mo. Sept. 13, 2023) ("There are no allegations that Plaintiff typed any information about herself, such as her name, address, phone number, or email address into data fields on Defendant's website. Plaintiff also does not allege that she shared any financial information, such as credit card or banking routing numbers."); *Straubmuller*, 2023 WL 5671615, at *4 ("Plaintiff further describes various types of 'highly sensitive' personal information that *could* be captured by Session Replay Code, including….credit card details.").

[171] *See e.g.*, Credit and Debit Card Receipt Clarification Act of 2007 (requiring account numbers printed on receipts have to be shortened to five digits in order to protect consumer privacy); *Greenstein v. Noblr Reciprocal Exch.*, 585 F. Supp. 3d 1220, 1227 (N.D. Cal. 2022) ("[T]he injury-in-fact requirement will be satisfied when highly sensitive personal data, such as social security numbers and credit card numbers, are inappropriately revealed to the public and increase the risk of immediate future harm to the plaintiff."); *Carlsen v. GameStop, Inc.*, 112 F. Supp. 3d 855, 862 (D. Minn. 2015) (finding no standing reasoning, "Plaintiff further fails to allege that Defendants disclosed any highly sensitive financial information such as credit card or social security data, but rather alleges that Defendants disclosed Plaintiff's Facebook ID and browsing patterns. This alone does not suffice to establish injury or imminent injury stemming from disclosure and differs substantially from injuries such as identity theft or costs to change account information."); *State v. Lunsford*, 226 N.J. 129, 131, 141 A.3d 270, 271 (2016) ("[A]ccount holders have a reasonable expectation of privacy in their bank and credit card records."); *Straubmuller*, 2023 WL 5671615,

at *4 ("Plaintiff further describes various types of 'highly sensitive' personal information that could be captured by Session Replay Code, including….credit card details.").

[172] We asked session replay Website Users' counsel whether Website Users are alleging Bass and Cabela's intercepted credit card information during oral argument. Session replay Website Users' counsel hesitated and eventually responded, "We are, your Honor, for the payment information, in order to make a payment." ECF No. 73 at 13:10-14:4. But Website Users do not allege the interception of credit card details. They instead rely on vague allegations session replay codes are *capable of* capturing credit card details. *See, e.g.*, ECF No. 53 at ¶¶ 73, 83, 85.

[173] *See Cook*, 2023 WL 5529772, at *4 ("That Ms. Cook's browsing activity here was anonymous is particularly significant and dooms any attempt to establish a concrete injury in fact."); *Massie*, 2022 WL 534468, at *5 ("Plaintiffs do not have a reasonable expectation of privacy over the anonymized data captured by the Session Replay software at issue here."); *James*, 2023 WL 7392285, at *7 ("To the extent *Lightoller* is read to hold non-anonymized information on, e.g., websites visited or search terms used is not sufficiently personal, the Court disagrees.").

[174] We are aware of several cases finding website visitors allege concrete harm arising from Facebook Tracking Pixel. We do not find these cases persuasive because they can be distinguished since they involve the private video viewing activity of website users *See, e.g., Carter v. Scripps Networks, LLC*, No. 22-2031, 2023 WL 3061858, at *1 (S.D.N.Y. Apr. 24, 2023) (finding concrete harm where Facebook allegedly tracked website visitors' video viewing activity through the Facebook Tracking Pixel); *Alex v. NFL Enterprises LLC*, No. 22-09239, 2023 WL 6294260, at *3 (S.D.N.Y. Sept. 27, 2023) ("Plaintiffs have sufficiently alleged they were injured when Defendants shared their private information and video watching data with Facebook without consent."); *Salazar v. Nat'l Basketball Ass'n*, No. 22-07935, 2023 WL 5016968, at *6 (S.D.N.Y. Aug. 7, 2023) ("Plaintiff's claim that Defendant purposefully shared his private viewing information with a third party without Plaintiff's knowledge or consent is akin to [intrusion upon seclusion]."); *Feldman v. Star Trib. Media Co. LLC*, No. 22-1731, 2023 WL 2388381, at *4 (D. Minn. Mar. 7, 2023) ("So described, this common law tradition bears a close relationship to Mr. Feldman's injury allegations: Mr. Feldman alleges that his video viewing history was his private concern, that the Star Tribune intruded by sharing this history with Facebook, and that this sharing would be offensive to a reasonable person. That seems enough at the motion-to-dismiss stage.").

[175] ECF No. 53 ¶¶ 47, 79-80.

[176] ECF No. 56 at 22 (citing *In re Google*, 806 F.3d 125).

[177] ECF No. 54-1 at 15.

[178] 2023 WL 7179807.

[179] *Id.* at *4.

[180] *Id.*

[181] *Id.*

[182] *Id.*

[183] ECF No. 56 at 41-42.

[184] ECF No. 53 ¶¶ 290-291.

[185] ECF No. 54-1 at 16.

[186] ECF No. 56 at 22.

[187] *Id.* at 23.

[188] *See Reilly v. Ceridian Corp.*, 664 F.3d 38, 44 (3d Cir. 2011) (dismissing for lack of standing despite allegations of "emotional distress"); *Heimbecker v. 555 Assocs.*, No. 01-6140, 2003 WL 21652182, at *14 (E.D. Pa. Mar. 26, 2003), *aff'd*, 90 F. App'x 435 (3d Cir. 2004) ("Plaintiff's allegations of emotional distress and damage to reputation are clearly insufficient to establish standing.").

[189] *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, No. 19-2904, 2021 WL 5937742, at *10 (D.N.J. Dec. 16, 2021) (rejecting attempts to "prop up their standing argument" on the theory a data breach diminished the value of their personal information).

[190] *Irvin* ECF No. 39 at 12.

[191] *Id.* at 14.

[192] *Irvin* ECF No. 47 at 8-9.

[193] 18 Pa. C.S. § 6111(i).

[194] *Irvin* ECF No. 20, ¶¶ 9, 69–70.

[195] *Barclift v. Keystone Credit Servs., LLC*, 585 F. Supp. 3d 748 (E.D. Pa. 2022).

[196] *Id.* at 751.

[197] *Id.* at 750.

[198] *Id.* at 758.

[199] *Id.*

[200] *Irvin* ECF No. 47 at 12-13.

[201] *Id.* at 9-10 (citing *Nickelodeon*, 827 F.3d at 274 (federal law); *Batts v. Gannett Co.*, 2023 WL 3143695, at *3 (E.D. Mich. Mar. 30, 2023) (Michigan law); *Salazar v. Nat'l Basketball Ass'n*, 2023 WL 5016968, at *5 (S.D.N.Y. Aug. 7, 2023) (Michigan law); and *Lin v. Crain Commc'ns, Inc.*, 2020 WL 248445, at *6 (E.D. Mich. Jan. 16, 2020) (Michigan law)).

[202] *Id.* at 10 (citing 18 Pa.C.S. § 6111(i)).

[203] *Id.*

[204] *TransUnion*, 141 S. Ct. at 2205 ("Congress's creation of a statutory prohibition or obligation and a cause of action does not relieve courts of their responsibility to independently decide whether a plaintiff has suffered a concrete harm under Article III.").

[205] *Farst*, 2023 WL 7179807, at *4 (citing *Boring v. Google Inc.*, 362 F. App'x 273, 280 (3d Cir. 2010)).

[206] Restatement (Second) of Torts § 652D cmt. a.

[207] See Cabela's Online Firearm Purchase Guidelines, https://www.cabelas.com/shop/en/online-firearm-purchaseguidelines#:~:text=Placing%20an%20Order%201%20Browse%20our%20available%20firearms,order%20will%20ship%20to%20the%20same%20store.%20

[208] *Farst*, 2023 WL 7179807, at *4.

[209] We found two state court cases in which individuals brought claims under section 6111(i) of the Uniform Firearms Act based on the alleged disclosure of confidential information. "Unlike federal courts, [Pennsylvania state courts] are open to resolve all controversies impacting the rights of Pennsylvanians and are vested by Article V, section 1 of the Pennsylvania Constitution with all judicial authority." *Firearm Owners Against Crime v. Papenfuse*, 261 A.3d 467, 496 n.6 (Pa. 2021). "[State court judges'] standing considerations account for many varied disputes that would fall short of constituting 'cases and controversies' in federal court." *Id.*

[210] ECF No. 53, Wherefore Clause, ¶ E; ¶¶ 221, 275, 296, 317, 339, 363, 381, 402, 421, 441.

[211] ECF No. 54-1 at 16-17.

[212] ECF No. 56 at 23.

[213] *TransUnion*, 141 S. Ct. at 2208 (citations omitted).

[214] *McNair v. Synapse Group Inc.*, 672 F.3d 213, 223 (3d Cir. 2012) (quoting *City of Los Angeles v. Lyons*, 461 U.S. 95, 105 (1983)).

[215] *Lyons*, 461 U.S. at 102; *O'Shea v. Littleton*, 414 U.S. 488, 495-96 (1974).

[216] *Lyons*, 461 U.S. at 102 (1983).

[217] 672 F.3d 213 (3d Cir. 2012).

[218] *Id.* at 215-19.

[219] *Id.* at 225.

[220] *Id.*

[221] 903 F.3d 278 (3d Cir. 2018).

[222] *Id.* at 282.

[223] *Id.* at 292.

[224] *Id.*

[225] *Id.* at 292-93.

[226] ECF No. 56 at 23.

[227] No. 20-3664, 2023 WL 5029899, at *7 (N.D. Cal. Aug. 7, 2023).

[228] *Id.* at *1.

[229] *Id.* at *7.

[230] *Id.*

[231] *Id.*

[232] *Id.* at *6.

[233] *See Kimca v. Sprout Foods, Inc.*, No. 21-12977, 2022 WL 1213488, at *10 (D.N.J. Apr. 25, 2022) (finding "[b]ecause [p]laintiffs . . . brought th[e] lawsuit, it is common sense that they are now aware of the alleged risks associated with the [allegedly deceptive product] and, thus, will not be deceived by [defendant's] marketing in the future").

[234] *McNair*, 672 F.3d at 225.

[235] *Id.* at 225 n.13.

[236] *McNair*, 672 F.3d at 223 (quoting *Lyons*, 461 U.S. at 105).

[237] *In re Flonase Antitrust Litig.*, 610 F. Supp. 2d 409, 413 (E.D. Pa. 2009) ("Unless at least one named Plaintiff can state a claim for relief under each count[,] Plaintiffs do not have standing to bring claims as part of a putative class action."). We dismiss with prejudice all claims under Count III (California Invasion of Privacy Act); Count IV (California statutory larceny); Count V (California Unfair Competition Law); Count VI (Maryland Wiretapping and Electronic Surveillance Act); Count VII (Maryland tort of invasion of privacy); Count X (Missouri Wiretap Act); Count XI (Missouri Merchandising Practices Act); and Count XII (Missouri common law intrusion upon seclusion).

[238] We dismiss without prejudice all claims under Count I (Federal Wiretap Act); Count II (Computer Fraud and Abuse Act), Count VIII (Massachusetts Wiretapping Statute), Count IX (Massachusetts Intrusion Upon Seclusion); Count XIII (Pennsylvania Wiretapping and Electronic Surveillance Control Act); Count XIV (Pennsylvania Intrusion Upon Seclusion); Count XV (Trespass to Chattels); Count XVI (Conversion to Chattels).